AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPLICANT(s):	Ruutu, J. and MA, J.		
SERIAL NO.:	09/456,263	ART UNIT:	2137
FILING DATE:	12/07/1999	EXAMINER:	Fields, C.
TITLE:	A METHOD FOR OPTIMIZING OF DATA TRANSMISSION		
ATTORNEY DOCKET NO.:	297-009078-US (PAR)		

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF

This is an appeal from the final rejection of the claims in the above-identified application. A Notice of Appeal was mailed on April 1, 2005.

I. REAL PARTY IN INTEREST

The real party in interest in this Appeal is:

Nokia Mobile Phones Ltd.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences regarding this application.

III. STATUS OF CLAIMS

Claims 1-11 pending in the application.

Claims 1-11 have been finally rejected.

The claims on appeal are 1-11.

IV. STATUS OF AMENDMENTS

There was no amendment filed under 37 CFR 1.116.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In brief, the present invention is related to optimization, e.g., minimizing lost data due to network congestion, of data transmission in TCP/IP networks, particularly to problems created by transmission of encrypted traffic (see page 4, line 37 to page 5, line 5). According to the invention, an indication of a TCP ACK being carried in the encrypted payload of a IP datagram is added in the IP header of the diagram (page 5, lines 15-19; page 9, lines 6-8, Fig. 17, 115 and 165). The indication may simply be a flag indicating the presence of a TCP acknowledgment (page 5, lines 27-28). The indication may also contain the acknowledgment number, which allows processing the

encrypted traffic based on the acknowledgment number (page 5, lines 25-31; page 9, lines 11 and 12). In IPv4 datagrams, the indication may be inserted as an extra option field (page 9, lines 16-18; page 5, lines 31 and 32). In IPv6 datagrams, the indication may be inserted as an extension header (page 10, lines 25 and 26; page 15, lines 32 and 33).

The invention defined by the independent claim is:

1. Method for processing IP traffic based on information within TCP headers carried in IP datagrams (Fig. 6, "TCP header"; page 5, lines 9-11), in which traffic at least some of the IP datagrams are encrypted (page 5, lines 11-13) characterized in that

if an IP datagram to be encrypted contains TCP header information used as a basis for the processing, at least an indication of the information on which the processing is based is placed into the header of said datagram (page 5, lines 15-19; Fig. 7, 115, 165; page 12, lines 8-21)

Claim 11 is the only claim which expressly recites a step.

11. A method according to claim 1, being used in congestion control in a TCP/IP network (p.1, 1.5; Fig. 4), characterized in that

the method comprises the step of delaying (Fig. 7, 130; p.12, 11. 7-13) the transmission of an encrypted IP datagram by a network element (Fig. 4, 20) if said encrypted IP datagram comprises an indication of a TCP acknowledgement and if said network element detects congestion in the network.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-11 are unpatentable under 35 USC 103(a) over Vidrasu in view of Ghani.

VII. ARGUMENT

A. Claim 1

The present invention solves the problem of congested networks by placing an indication on which processing is based into the header of a datagram.

Please notice in Vidrascu et al column 1, lines 57-64:

"For this purpose, the invention is a method of enciphering messages transmitted between networks interconnected via highways using a specified network protocol, characterised in that the messages are enciphered while keeping the *"header"* part of the message plain (not enciphered) allowing its routing via the highways..."

It is noted that in determining obviousness a consideration is what a reference suggests to one of ordinary skill in the art. The CAFC has stated:

> In determining whether such a suggestion can fairly be gleaned from the prior art, the full field of the invention must be

> considered; for the person of ordinary skill is charged with knowledge of the entire body of technological literature, including that which might lead away from the claimed invention. The Commissioner argues that since the PTO is no longer relying on Farmer or the Bacon and Farmer article, the applicant is creating a "straw man". It is indeed pertinent that these references teach against the present invention. Evidence that supports, rather than negates, patentability must be fairly considered (emphasis added). See In re Dow Chemical, 5 USPQ2d 1529, 1531-2, 837F.2d 469, 473, (CAFC 1988).

Here Vidrascu expressly teaches away from the present invention by stating that the header is not enciphered. Many other cases are in accord, see Singh v. Brake, 317 F.3d 1334, 1346, 65 USPQ2d 1641 (CAFC 2003); Gillette Co. v. S.C. Johnson & Sons, Inc., 919 F2d 720,724, 16 USPQ2d 1923, 1927 (CAFC 1990); In re Haruna 249 F.3d 1327, 1335, 58 USPQ2d 1517 (CAFC 2001).

The Examiner has looked at column 12, lines 1-20, but, for instance, the Finnish patent office in its office action has stated that Vidrascu is actually an 'A' publication (background only) and not an obstacle at all for patenting in Finland. While the USPTO is independent of the Finnish patent office, its comments are useful. According to the Finnish patent office, there is described in Vidrascu a method and device which is used in enciphering messages between two networks. The networks use

IP-protocol in the network layer and in the transfer layer TCP- or UDP-protocol. The Finnish patent office further states, that it is characteristic that the IP-header is not enciphered. Instead, at least a part of TCP- or UDP headers are enciphered. The Finnish office mentions parts of the Vidrascu, namely column 1, line 36, column 4, line 44, column 6, lines 18-46, column 11, lines 11—20, claims 1-12. Thus the Finnish patent office has dealt with the same reference, but ranked it as an A publication.

Further, it us respectfully submitted that the Examiner tries to combine two irrelevant techniques to result in the invention.

So, if one still looks at the figure 12, there is an indication that 'part of TCP or UDP header' as has been mentioned in col. 10, lines 49-53, but having a reference to items 84 and 85, which in figures 10 and 11 are related to checksum as in Vidrascu. There is no IP in the figure 12 at all. If an IP item is searched from Vidrascu, such is indicated by a reference numeral 75, whereas UDP or TCP by 76 (col. 10, line 60).

In addition, in col. 2, lines 37-40, it is indicated that a goal of Vidrascu is to provide 64-bit divisional strings. If now one looks also at col. 1, lines 60-62, a skilled man in the art immediately knows that the techniques used in Vidrascu have nothing to do with encrypting the IP header as in the currently claimed invention.

If one now additionally looks at col. 2, lines 41-63, a skilled man in the art can see the function of CHEKSUM. The abstraction

level for the opinions in the office action seems to be so high, that if something is encrypted, there must be a way or a key to do the opposite. How such is implemented with the known techniques in the references and how in the current application using a different way is not stated.

In the description of col. 8, line 38, the item 94 indeed may be involved with retrieval of an encryption key, but taken from a totally different place than in the current application. It has actually nothing to do with the presently claimed feature of "indication of the information on which the processing is based". If a skilled man in the art looks at Vidrascu col. 8, lines 31-44, it can read on what the Vidrascu teachings of the techniques are based on, but the text indicate in a different manner from that of the present invention. The text relates to SERVER associated keys. Thus a skilled man in the art immediately knows that the techniques in Vidrascu do not relate to the processing. Vidrascu seems to only relate to a key pair between the servers.

In Ghani the congestion bit is not used for encryption. It is said in Ghani, that the techniques therein are aimed at congestion bits, and thus they do not have any relevance to the current invention. If we now also look at the location where Ghani puts his bit, it seems to be into the IP header, not into the TCP, UDP header. Therefore, if an attempt were made to combine Vidrascu and Ghani, a skilled man in the art would be totally at a loss at what to do. If Vidrascu were considered to teach to encrypt TCP/UDP header and Ghani to put an indication of the congestion into IP, the teachings won't combine at all.

The teaching of Vidrascu still tells not to encrypt the IP-header "...while keeping the 'header' part of the message plain (not enciphered) allowing its routing..."

Thus combining these references results in an inoperable device. This is indicative of non-obviousness, see In re Sponnoble, 405 F.2d 578,587, 160 USPQ 237, 244, 56 CCPA 823 (1969).

As stated in In re Gordon, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (CAFC 1984):

> Indeed, if the French apparatus were turned up-side down, it would be rendered inoperable for its intended purpose. ...French teaches away from the boards's proposed modification.

The final rejection maintains that applicants argue Vidrascu's does not teach IP at all. That is actually not the case, and the statement in the final rejection is irrelevant.

In the figure 12 texts, applicants have shown that there is no IP at all. However, in that part of the text relating to the figure, the items 84 and 85 therein are not to IP related, but instead to TCP or UDP header (76, 77), please see Col. 10, lines 49-53, to see what it is all about. The IP header totally passes the encipherment part. It is the part of the teachings of Vidrascu that the examiner has neglected from the document, which is the part of it applicants are actually pointing out as indicating differences. Col. 11, lines 3-7, tell what parts are encrypted. The IP-protocol is NOT-ENCRYPTED therein at all! Only the TCP or UDP header is encrypted.

To summarize, in Ghani congestion bits seem to be put into the IP header and Vidrascu teaches that what was put into the IP would not be encrypted at all because otherwise the routing does not work well. There is no teaching at all to the skilled man in the art to combine these references, and even if there were such a teaching, the result is not the present invention.

Claim 1 recites "if an IP datagram to be encrypted contains TCP header information used as a basis for the processing, at least an indication of the information on which the processing is based is placed into the header of said datagram." This is not in the references.

Thus even if the references are somehow combined, the result is not the claimed invention. Thus the rejection of claims 1-11 under 35 USC 103 should be withdrawn.

B. Claim 2

Claim 2 recites that if an IP datagram to be encrypted has a TCP acknowledgement, an indication of the acknowledgement is placed into the header of the datagram. The Examiner has cited Vidrascu (col. 12, sic 11?, ll. 1-20; & Figs. 9 & 12) and Ghani (col. 6, ll. 26-54; & Fig. 4). However, Vidrascu does not mention acknowledgements, and while Ghani mentions acknowledgements, there is no disclosure of placing them in the header. Thus even if the references are somehow combined, the result is not the invention of claim 2.

For this additional reason, claim 2 is patentable.

C. Claim 3

Claim 3 recites placing a copy of at least the information on which processing is based into the header. The references disclose absolutely nothing about placing such a copy into the header. Thus even if the references are somehow combined, the result is not the invention of claim 3.

For this additional reason, claim 3 is patentable.

D. Claim 4

Claim 4 adds to claim 3 that the placing comprises placing all information. The references disclose nothing about this. Thus even if the references are somehow combined, the result is not the invention of claim 4.

For this additional reason, claim 4 is patentable.

E. Claim 5

Claim 5 adds to claim 3 that a copy of a TCP acknowledgement number is placed into the header. The references do not disclose this feature. Thus even if they are somehow combined, the result is not the invention of claim 5.

For this additional reason, claim 5 is patentable.

F. Claim 6

Claim 6 recites that a copy of the contents of the window sized field of a TCP header is placed into the header. The Examiner cites Fig. 10 of Vidrascu for this, but there is no disclosure of such a copy in the header in this figure. The description (col. 11, 11. 3 & 4) also lacks this feature. Similarly, Ghani fails to disclose this. Thus even if the references are somehow combined, the result is not the invention of claim 6.

For this additional reason, claim 6 is patentable.

G. Claim 7

Claim 7 recites that if the datagram is an IPV6 datagram, the indication is placed in the options field. The Examiner has cited Fig. 9 of Vidrascu. However, this figure discloses nothing about such an indication or an options field. Similarly, Ghani does not make such a disclosure. Thus even if the references are somehow combined, the result is not the invention of claim 7.

For this additional reason, claim 7 is patentable.

H. Claim 8

Claim 8 recites that if the datagram is an IPV6 datagram, the indication is in an extension header. The Examiner cites Fig. 11 of Vidrascu. However, this figure discloses nothing about such an indication or an extension header. Similarly, neither does

Ghani make such a disclosure. Thus even if these references are somehow combined, the result is not the invention of claim 8.

For this additional reason, claim 8 is patentable.

I. Claim 9

Claim 9 recites that the intermediate network modifies the copy of the information on which processing is based. The Examiner cites nothing in either reference as disclosing this feature. Thus even if the references are combined, the result is not the invention of claim 9.

For this additional reason, claim 9 is patentable.

J. Claim 10

Claim 10, which depends from claim 9, recites that the destination element was the modified copy of the information instead of the encrypted version. The Examiner cites nothing in either reference as disclosing this feature. Thus even if the references are somehow combined, the result is not the invention of claim 10.

For this additional reason, claim 10 is patentable.

K. Claim 11

Claim 11 recites delaying the transmission of the IP datagram if the encrypted datagram comprises an acknowledgement and if there is congestion in the network. The Examiner has cited nothing in

either reference for this. Thus even if the references are somehow combined, the result is not the invention of claim 11.

For this additional reason, claim 11 is patentable.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, a reversal of the rejection of claims 1-11 is respectfully requested from this Honorable Board.

A check in the amount of $500 is enclosed herewith for the appeal brief fee. The Commissioner is hereby authorized to charge payment for any additional fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Henry I. Steckler
Reg. No.: 24,139

May 17, 2005
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date indicated below as first class mail in an envelope addressed to the Board of Patent Appeals and Interferences United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450,

Date: 5/12/05

Signature: Rosanna Belencia
Rerson Making Deposit

VIII. CLAIM APPENDIX

The texts of the claims involved in the appeal are:

1. Method for processing IP traffic based on information within TCP headers carried in IP datagrams, in which traffic at least some of the IP datagrams are encrypted, characterized in that

if an IP datagram to be encrypted contains TCP header information used as a basis for the processing, at least an indication of the information on which the processing is based is placed into the header of said datagram.

2. A method according to claim 1, characterized in that if an IP datagram to be encrypted contains a TCP acknowledgment, an indication of the acknowledgment is placed into the header of said datagram.

3. A method according to claim 1, characterized in that said placing of at least an indication into the header of said datagram comprises placing a copy of at least the information on which the processing is based into the header of said datagram.

4. A method according to claim 3, characterized in that said placing of at least an indication into the header of said datagram comprises placing of all information of a TCP header into the header of said datagram.

5. A method according to claim 3, characterized in that a copy of a TCP acknowledgement number is placed into the header of said datagram.

6. A method according to claim 3, characterized in that a copy of the contents of the window size field of a TCP header is placed into the header of said datagram.

7. A method according to claim 1, characterized in that if said datagram is an IPv4 datagram, said at least an indication is placed in an options field of said datagram.

8. A method according to claim 1, characterized in that if said datagram is an IPv6 datagram, said at least an indication is placed in an extension header in said datagram.

9. A method according to claim 3, in which method

-a source network element generates IP datagrams,

-an intermediate network element forwards the IP datagrams to a destination network element, and

-the destination network element receives the IP datagrams,

characterized in that

the intermediate network element modifies said copy of the information on which the processing is based.

10. A method according to claim 9, characterized in that

said destination network element uses said modified copy of the information instead of the encrypted version of the information carried as the payload of the IP datagram.

11. A method according to claim 1, being used in congestion control in a TCP/IP network, characterized in that

the method comprises the step of delaying the transmission of an encrypted IP datagram by a network element, if said encrypted IP datagram comprises an indication of a TCP acknowledgement and if said network element detects congestion in the network.

IX. EVIDENCE APPENDIX

Not Applicable

X. RELATED PROCEEDINGS APPENDIX

Not Applicable